UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/530,638	11/08/2005	Andrew Gordon Williams	562492003900	7507

20872 7590 05/22/2009

MORRISON & FOERSTER LLP
425 MARKET STREET
SAN FRANCISCO, CA 94105-2482

EXAMINER	
KELLEY, STEVEN SHAUN	
ART UNIT	PAPER NUMBER
2617	
MAIL DATE	DELIVERY MODE
05/22/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/530,638	WILLIAMS ET AL.	
	Examiner	Art Unit	
	STEVEN KELLEY	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 April 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30 and 32-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30 and 32-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Detailed Action

Claims 1-30 and 32-45 have been examined. Claim 31 has been cancelled.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 32-45 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. There is no support in the specification for a computer readable medium which can "*provide* a SGSN" and can "*provide* a RADIUS server" as recited. Executing stored instructions can not "provide" the devices as recited in claim 32.

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 29-30 and 32-45 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 29 and 30 are unclear and/or inaccurate as to how a RADIUS server (or SGSN in claim 30) can be configured to

"*provide* a RADIUS server" and "*provide* a SGSN" (as recited in the method of claim 15). It is unclear and/or inaccurate as to how "executing instructions" can "*provide*" a SGSN and RADIUS server, as recited in claim 32.

Claim Rejections - 35 USC § 103

5. Claims 1-3, 15-17, 29-30 and 32-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over WO 02/011467 to Jones et al (hereinafter "Jones") in view of 2003/0051041 to Kalavade et al. (hereinafter "Kalavade").

Regarding claim 1, which recites a system for use of internet authentication technology to provide UMTS authentication, the system comprising a Serving GPRS Node (SGSN) in a UMTS network and a RADIUS server, Jones discloses a Serving GPRS Node (SGSN) 27 connected to a RADIUS Server 34. Jones further teaches "the SGSN 27 and the RADIUS server 34 being adapted to support signaling there between" as described with reference to Fig. 3, for example. Jones teaches authenticating user equipment connections in the RADIUS server 34 for wireless access, but Jones does not disclose "whereby authentication of a User Subscriber Identity Module (USIM) is performed by the RADIUS Server," as recited in claim 1. In an analogous art, Kalavade teaches authenticating roaming wireless devices with the use of a Converged Billing Gateway (CBG) server 10, where the wireless devices include a Subscriber Identity Module (SIM). Kalavade discusses the integration of RADIUS with the CBG server 10 in sections [0204] to [0213]. In section [0209] Kalavade recites "the CBG functions as a remote RADIUS server 10" and "in some cases the CBG may do the additional SIM

check or the phone check to get authentication information". In section [0213] Kalavade recites "Note that if no RADIUS server is associated with the hotspot, then the CBG can provide the complete authentication as well as functioning as the RADIUS server." Therefore, in order to efficiently and cost effectively provide authentication functions in existing network equipment (without requiring additional authentication servers and equipment as taught in Kalavade), it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the RADIUS server of Jones to perform authentication of USIM data within the RADIUS server, as recited in claim 1.

Regarding claim 15, which recites a method for use of internet authentication technology to provide UMTS authentication, the method comprising providing Serving GPRS Node (SGSN) in a UMTS network and providing RADIUS server, Jones teaches a Serving GPRS Node (SGSN) 27 connected to a RADIUS Server 34. Jones further teaches "signaling between the SGSN 27 and the RADIUS server 34" as described with reference to Fig. 3, for example. Jones teaches authenticating user equipment connections in the RADIUS server 34 for wireless access, but Jones does not disclose "that authentication of a User Subscriber Identity Module (USIM) is performed in the RADIUS Server," as recited in claim 15. In an analogous art, Kalavade teaches authenticating roaming wireless devices with the use of a Converged Billing Gateway (CBG) server 10, where the wireless devices include a Subscriber Identity Module (SIM). Kalavade discusses the integration of RADIUS with the CBG server 10 in sections [0204] to [0213]. In section [0209] Kalavade recites "the CBG functions as a remote RADIUS server 10" and "in some cases the CBG may do the additional SIM

check or the phone check to get authentication information". In section [0213] Kalavade recites "Note that if no RADIUS server is associated with the hotspot, then the CBG can provide the complete authentication as well as functioning as the RADIUS server." Therefore, in order to efficiently and cost effectively provide authentication functions in existing network equipment (without requiring additional authentication servers and equipment as taught in Kalavade), it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the RADIUS server of Jones to perform authentication of USIM data within the RADIUS server, as recited in claim 15.

Regarding claim 32, see the rejection of claim 15 above. Claim 32 recites the same steps recited in claim 15 as being performed by computer executable instructions stored on a computer readable storage medium. Regarding the "computer executable instructions stored on a computer readable storage medium", Jones teaches on page 12, that the "roaming functions (as would be performed by RADISU servers) will typically be carried out in computer programs or routines in software".

Regarding claims 2, 16 and 33 which recite "wherein the SGSN is integrated with a RNC within an INC", see Fig. 1 of Jones, which shows the SGSN (27) that is integrated with a RNC (26) within an INC (24), as recited.

Regarding claims 3, 17 and 34, which recite "wherein the UTMS network comprises a UTRAN network", see for example the Background, the Detailed Description and Fig. 1 of Jones, which teach this recited feature.

Regarding claims 29 and 30, the combination of Jones and Kalavade teach a RADIUS server and SGSN to perform the functions as recited in claim 15.

5. Claims 4-14, 18-28 and 35-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones and Kalavade as applied to claims 1, 15 and 32 above, and further in view of the "standards documents [1]-[5]" referred to in the instant application.

Regarding claims 4, 18 and 35, which recite "wherein the SGSN is configured to send an Access-Request RADIUS message to request a UMTS Authentication Vector from the RADIUS server", both Jones and Kalavade teach using Access Request RADIUS messages. See for example, pages 11-12 of Jones and section [0207] of Kalavade which teaches that "The RADIUS client sends an Access Request message to the RADIUS server". Kalavade teaches in section [0218] of using "authorization vectors for SIM based authorization", however, does not explicitly teach requesting a "UMTS Authentication Vector from the RADIUS server" as recited.

As described and referenced on pages 1-3 (and additionally throughout) of the instant specification, "standards documents 1-5" describe the signaling protocols for UMTS authentication and RADIUS protocols. Page 10 of the instant application cites "standards document [3]" as teaching the use of a "UMTS Authentication Vector".

Therefore, as Jones teaches (on page 11) of "modifying the basic code format (of RADIUS protocol messages 41 and 42 as shown in Fig. 3) for each particular function", and Kalavade teaches the use of authentication vectors, it would have been obvious to modify the RADIUS server of Jones to provide a UMTS Authentication Vector (as taught by the "standards documents") as recited, in order to provide a conventional (and compatible) authentication response signal to the SGSN.

Regarding claims 5, 19 and 36, which recite "wherein the RADIUS Server is configured to generate authentication and keying material so as to authenticate a USIM within a UMTS UE, according to UMTS standards", Jones and Kalavade do not explicitly teach this feature as recited.

As described and referenced on pages 5-6 of the instant specification, "standards documents 1-4" describe the signaling protocols for UMTS authentication, which include keying material, such as a value "k" described in the last paragraph on page 5, for example.

Therefore, as Jones and Kalavade teach the conventionality of configuring devices to be compatible with additional standard protocols, it would have been obvious to modify the RADIUS server of Jones to generate authentication and keying material so as to authenticate a USIM within a UMTS UE, according to UMTS standards (as taught by the "standards documents") as recited, in order to provide a conventional UMTS authentications.

Regarding claims 6, 20 and 37, which recite "wherein the RADIUS Server is configured to implement the MILENAGE algorithm", Jones and Kalavade do not explicitly teach using a MILENAGE algorithm as recited.

As described and referenced on pages 1-3 (and additionally throughout) of the instant specification, "standards documents 1-5" describe the signaling protocols for UMTS authentication and RADIUS protocols. Page 2 of the instant application cites "standards documents [3] and [4]" as teaching the use of a "MILENAGE algorithm".

Therefore, as Jones and Kalavade teach the conventionality of configuring devices to be compatible with additional standard protocols and programs, it would have been obvious to modify the RADIUS server of Jones to be configured to implement a MILENAGE algorithm (as taught by the "standards documents") as recited, in order to provide a conventional UMTS authentication.

Regarding claims 7, 21 and 38, which recite "wherein the RADIUS Server is configured to generate, using anti-replay-attack dynamic data, a UMTS Authentication Vector, for use by the SGSN", Jones and Kalavade do not explicitly teach this feature as recited.

As described and referenced on pages 1-3 (and additionally throughout) of the instant specification, "standards documents 1-5" describe the signaling protocols for UMTS authentication and RADIUS protocols. Page 10 of the instant application cites "standards document [3]" as teaching the use of a "UMTS Authentication Vector", and page 14 of the instant application cites "standards document [2]" as teaching the use of anti-replay-attack data.

Therefore, as Jones and Kalavade teach the conventionality of configuring devices to be compatible with additional standard protocols, it would have been obvious to modify the RADIUS server of Jones to provide a UMTS Authentication Vector (as taught by the "standards documents") using anti-replay attack data as recited, in order to provide a conventional (and compatible) authentication response to the SGSN.

Regarding claims 8, 22 and 39, which recite "wherein the RADIUS Server is configured to support dynamic sequence number (SQN)", Jones and Kalavade do not explicitly teach this feature as recited.

As described and referenced on pages 1-3 (and additionally throughout) of the instant specification, "standards documents 1-5" describe the signaling protocols for UMTS authentication and RADIUS protocols. Pages 5-6 of the instant application cites "standards documents 1-4", used with the MILENAGE algorithm, as supporting/using dynamic sequence number (SQN).

Therefore, as Jones and Kalavade teach the conventionality of configuring devices to be compatible with additional standard protocols and programs, it would have been obvious to modify the RADIUS server of Jones to support SQN (as taught by the "standards documents") as recited, in order to provide a conventional (and compatible) authentication response signal to the SGSN.

Regarding claims 9, 23 and 40, which recite "wherein the RADIUS Server is configured to generate a UMTS Authentication Vector in a RADIUS attribute within an Access-Accept RADIUS message for sending to the SGSN", both Jones and Kalavade teach using Access Request RADIUS messages. See for example, pages 11-12 of Jones and section [0207] of Kalavade which teaches that "The RADIUS client sends an Access Request message to the RADIUS server". Kalavade teaches in section [0218] of using "authorization vectors for SIM based authorization", however, does not explicitly teach generating a "UMTS Authentication Vector" as recited.

As described and referenced on pages 1-3 (and additionally throughout) of the instant specification, "standards documents 1-5" describe the signaling protocols for UMTS authentication and RADIUS protocols. Page 10 of the instant application cites "standards document [3]" as teaching the use of a "UMTS Authentication Vector" and pages 10-11 cite "standards document [5]" as teaching the Access-Accept RADIUS message.

Therefore, as Jones teaches (on page 11) of "modifying the basic code format (of RADIUS protocol messages 41 and 42 as shown in Fig. 3) for each particular function", and Kalavade teaches using authentication vectors, it would have been obvious to modify the RADIUS server of Jones to provide a UMTS Authentication Vector (as taught by the "standards documents") as recited, in order to provide a conventional (and compatible) authentication response signal to the SGSN.

Regarding claims 10, 24 and 41, which recite "wherein the SGSN is configured to receive a UMTS Authentication Vector in a RADIUS Access-Accept message", both Jones and Kalavade teach using Access Request RADIUS messages. See for example, pages 11-12 of Jones and section [0207] of Kalavade which teaches that "The RADIUS client sends an Access Request message to the RADIUS server". Kalavade teaches in section [0218] of using "authorization vectors for SIM based authorization", however, does not explicitly teach receiving a "UMTS Authentication Vector" as recited.

As described and referenced on pages 1-3 (and additionally throughout) of the instant specification, "standards documents 1-5" describe the signaling protocols for UMTS authentication and RADIUS protocols. Page 10 of the instant application cites

"standards document [3]" as teaching the use of a "UMTS Authentication Vector" and pages 10-11 cite "standards document [5]" as teaching the Access-Accept RADIUS message.

Therefore, as Jones teaches (on page 11) of "modifying the basic code format (of RADIUS protocol messages 41 and 42 as shown in Fig. 3) for each particular function", and Kalavade teaches using authentication vectors, it would have been obvious to modify the SGSN of Jones to receive a UMTS Authentication Vector (as taught by the "standards documents") as recited, in order to provide a conventional (and compatible) authentication response signal to the SGSN.

Regarding claims 11, 25 and 42, which recite "wherein the SGSN is configured to send information to re-synchronize anti-replay-attack information within the USIM with the RADIUS Server", Jones and Kalavade do not explicitly teach this feature as recited.

As described and referenced on pages 1-3 (and additionally throughout) of the instant specification, "standards documents 1-5" describe the signaling protocols for UMTS authentication and RADIUS protocols. Page 14 of the instant application cites "standards document [2]" as teaching the use of "anti-replay-attack information".

Therefore, as Jones and Kalavade teach the conventionality of configuring devices to be compatible with additional standard protocols, it would have been obvious to modify the SGSN of Jones to provide information to re-synchronize anti-replay-attack information (as taught by the "standards documents") as recited, in order to provide authentication information to the RADIUS server, as is conventional.

Regarding claims 12, 26 and 43, which recite "wherein the SGSN is configured to send a UMTS-Resynchronization token attribute in the Access-Request RADIUS message", Jones and Kalavade do not explicitly teach this feature as recited.

As described and referenced on pages 1-3 (and additionally throughout) of the instant specification, "standards documents 1-5" describe the signaling protocols for UMTS authentication and RADIUS protocols. Page 10 of the instant application cites "standards document [3]" as teaching the use of a "UMTS-Resynchronization token attribute" and pages 10-11 cites "standards document [5]" as teaching the use of the "Access-Request RADIUS message".

Therefore, as Jones teaches (on page 11) of "modifying the basic code format (of RADIUS protocol messages 41 and 42 as shown in Fig. 3) for each particular function", it would have been obvious to modify the SGSN of Jones to provide a UMTS Authentication Vector (as taught by the "standards documents") as recited, in order to provide a conventional (and compatible) signal to the RADIUS server.

Regarding claims 13, 27 and 44, which recite "wherein the RADIUS Server is configured to reset anti-replay attack dynamic data in-line with the USIM in response to the data received in the UMTS-Resynchronization-Token", Jones and Kalavade do not explicitly teach this feature as recited.

As described and referenced on pages 1-3 (and additionally throughout) of the instant specification, "standards documents 1-5" describe the signaling protocols for UMTS authentication and RADIUS protocols. Page 10 of the instant application cites "standard document [3]" as teaching the use of a "UMTS-Resynchronization-Token" and

page 14 of the specification cites "standards document [2]" as teaching the use of "anti-replay attack dynamic data".

Therefore, as Jones teaches (on page 11) of "modifying the basic code format (of RADIUS protocol messages 41 and 42 as shown in Fig. 3) for each particular function", it would have been obvious to modify the RADIUS server of Jones to reset anti-replay attack dynamic data (as taught by the "standards documents") as recited, in order to provide secure authentication processes.

Regarding claims 14, 28 and 45, which recite "wherein the RADIUS Server is configured to implement the MILENAGE algorithm", Jones and Kalavade do not explicitly teach using a MILENAGE algorithm as recited.

As described and referenced on pages 1-3 (and additionally throughout) of the instant specification, "standards documents 1-5" describe the signaling protocols for UMTS authentication and RADIUS protocols. Page 2 of the instant application cites "standards documents [3] and [4]" as teaching the use of a "MILENAGE algorithm".

Therefore, as Jones and Kalavade teach the conventionality of configuring devices to be compatible with additional standard protocols, it would have been obvious to modify the RADIUS server of Jones to be configured to implement a MILENAGE algorithm (as taught by the "standards documents") as recited, in order to provide a conventional UMTS authentication.

Response to Arguments

Applicant's arguments filed 4-15-09 have been fully considered but they are not persuasive. Applicant's argue the single point that Kalavade does not teach "that the USIM authentication is performed in the RADIUS server". The Examiner agrees and emphasizes that (contrary to Applicant's allegation on page 10 of the response that "The Examiner points to Kalavade, in particular sections [0209] and [0213], as disclosing this element") the First Office Action sets forth that the teachings of Kalavade do not explicitly disclose this feature, however, the teachings of Kalavade do render obvious modifying a RADIUS server (such as disclosed in Jones) to produce this feature. As was described in the First Office Action, Kalavade teaches that the CBG 10 may be configured to function as a RADIUS server and additionally, the CBG 10 may be configured to perform SIM authentication. The Office Action sets forth that if one of ordinary skill can configure a CBG to perform both RADIUS and SIM authentication functions, one of ordinary skill would (obviously) conclude that a RADIUS server may be configured to perform SIM authentication functions. Applicant's remarks are therefore not persuasive, as the remarks address the references individually and do not address the references in combination, i.e., why it would not be obvious to one of ordinary skill to modify the RADIUS server of Jones in view of the teachings of Kalavade to perform USIM authentication.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Steven Kelley whose telephone number is (571) 272-5652. The examiner can normally be reached on Monday-Friday, 9AM to 5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lester Kincaid can be reached on (571) 272-7922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/SSK/

/Lester Kincaid/
Supervisory Patent Examiner, Art Unit 2617